Secure-IC's answer to Side-Channel Security Evaluation Labs Call

March 15, 2022

Abstract

Secure-IC offers its Analyzr platform for the evaluation of NIST LWC HW candidates finalists.

1 Equipment and Software Used

The detail of the equipments is provided in Tab. 1.

2 Supported Leakage Assessment Methods

The leakage assessment methods supported by Secure-IC are listed in Tab. 2.

3 Supported Attacks

Secure-IC does not perform any key extraction. Analyzr is to be used in a DevSecOps context. The purpose of Analyzr platform is to help designers to identify leaks.

4 Ability to generate and publish raw measurements to be analyzed by other groups

Analyzr can export data in HD5 format, as required by Annex C of ISO/IEC 20085-1:2019, entitled "Data exchange and storing technologies".

Table 1: Equipment and Software Used

	Item	**Secure-IC's response**
(a)	General type of platform	Secure-IC Analyzr, documented here: https://www.secure-ic.com/solutions/analyzr/
(b)	FPGA board	Sakura-G
(c)	FPGA model	Xilinx Spartan-6 board
(d)	Oscilloscope	Tektronix, MSO64 (6 GHz bandwidth, 25 G sample/s)
(e)	Electromagnetic probes	Either probes provided by Langer, or home-made EM probes
(f)	Measurement options	As offered by Analyzr
(g)	Are sampling clock and design-under-evaluation clock synchronized?	No
(h)	Names and versions of programs used for evaluating side-channel resistance	Analyzr

Table 2: Equipment and Software Used

	Item	**Secure-IC's response**
(a)	Type of the method	Tests specified in ISO/IEC 17825:2016
(b)	Approximate number of traces used in evaluations of authenticated ciphers	100,000 traces
(c)	Typical clock frequency of the device-under-evaluation	100 MHz
(d)	Sampling frequency and resolution	Up to 25 Gsample/s
(e)	Graphical representation of results	Representation specified in ISO/IEC 17825:2016

5 Support for side-channel analysis as service, with the feedback provided to designers of protected implementations during the development process

Secure-IC offers an Evaluation as a Service (EaaS) by its Think Ahead business line.

6 Short description of the personnel and its qualifications

Secure-IC personnel is specialist in side-channel evaluation. Evaluators hold a PhD in embedded cyber-security, and use Analyzr tool on a regular basis. A recent paper leveraging Analyzr is for instance [1].

7 Intended period of the lab operation

Secure-IC's lab is available during the evaluation of the LWC HW candidates.

8 Contact information

Please contact:

- Sylvain Guilley, `sylvain.guilley@secure-ic.com` — CTO,
- Khaled Karray, `khaled.karray@secure-ic.com` — Threat Analysis Business Line Director.

References

[1] Sofiane Takarabt, Sylvain Guilley, Youssef Souissi, Khaled Karray, Laurent Sauvage, and Yves Mathieu. Formal Evaluation and Construction of Glitch-resistant Masked Functions. In *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2021, Tysons Corner, VA, USA, December 12-15, 2021*, pages 304–313. IEEE, 2021.